

CAL FIRE DESKTOP AND MOBILE COMPUTING POLICY (No.24 December 2009)

0960

CAL FIRE DESKTOP AND MOBILE COMPUTING (No.24 December 2009)

0960.1

The California Department of Forestry and Fire Protection (CAL FIRE) has adopted the following policy regarding the acquisition, tracking, and use of Information Technology (IT) assets for desktop and mobile computing. Under delegated authority from Department of Finance and SAM section 4989 through 4989.3, CAL FIRE may acquire desktop and mobile computing commodities to support the Department's program functions and business needs.

PURPOSE

960.1.2

(No.24 December 2009)

This policy establishes standards for the use and management of desktop and mobile computing within the CAL FIRE, specifically:

- Ensures that the use of desktop and mobile computing is consistent with the Department's information management strategy, state standards, and information technology infrastructure;

- Coordinates with information technology applications including commercial off-the-shelf software and applications developed in-house on the same desktop and mobile computing configuration to maintain compatibility and functionality;

- Establishes an appropriate Department policy structure for the justification, acquisition, accountability, inventory, and use of desktop and mobile computing assets;

- Promotes the identification of cost-effective opportunities when using desktop and mobile computing assets to support the accomplishment of the CAL FIRE mission and program objectives;

- Establishes an appropriate policy structure for the continued maintenance, support, training, scanning, and upgrade of implemented desktop and mobile computing configurations; and

- Ensures the integrity, access, and security of automated files and information systems; and that program operations are compliant with all applicable provisions of SAM as well as applicable standards, and are aligned with the Department's Operational Recovery Plan.

SCOPE OF THE DESKTOP AND MOBILE COMPUTING POLICY

960.1.3

(No.24 December 2009)

State Administrative Manual (SAM) Section 4989.2 excludes the following activities from the Desktop and Mobile Computing Policy. These exclusions must be treated in accordance with SAM Sections 4819.3 through 4819.42. <http://sam.dgs.ca.gov/TOC/4800/4819.3.htm>

IT Projects – As defined in SAM Section 4819.2, beyond the acquisition, installation, and operation of DMCP commodities as defined in this policy. The acquisition of desktop and mobile computing commodities required for an IT project, whether reportable or delegated, must be included within the project scope and acquired under the approved project's authority. Use of this policy to circumvent IT project reporting requirements or to make an otherwise reportable project fall within delegated thresholds is expressly prohibited.

Budget Actions – Any acquisition, maintenance, or support of desktop and mobile computing commodities which requires a Budget Change Proposal, a Budget Revision, or other budget action is not covered by the Desktop and Mobile Computing Policy. However, this policy may be used to acquire the standard complement of desktop and mobile computing commodities as approved by Finance for new positions.

Specialized or Single-Purpose Systems – Acquiring any specialized, single-purpose, non-modifiable system, such as computer-aided design systems, desktop publishing systems, programmer workbench systems, or artificial intelligence systems is excluded from the policy. However, software-based applications used on a general-purpose personal computer may be covered by the policy. For example, desktop publishing employing word processing, graphics, and page layout software packages on a general-purpose personal computer falls within this policy; desktop publishing employing a specialized computer system that has been developed and marketed for the sole purpose of doing desktop publishing does not. A specialized, single-purpose system that allows some connectivity to an agency's existing systems, such as electronic mail, is still considered a specialized or single-purpose system for the purposes of this policy.

Infrastructure or Platform Migration – Acquisitions associated with or mandated by a change in an agency's standard technical architecture for servers, desktops and/or mobile computing platforms are excluded from the policy. Migrating to a newer version within the existing standard's product family is not considered an infrastructure or platform migration.

Wide Area Networks (WAN) – The acquisition, maintenance, or support of desktop and mobile computing commodities specifically to install or operate a WAN are excluded from the policy. These activities for WANs are considered IT projects, or components of IT projects, for the purposes of this policy. However, upgrading the capacity of a previously approved WAN project may fall within the definition of a previously approved project. (See SAM Section 4819.2: "Previously Approved Effort/Project".)

Units wishing to initiate information technology projects outside of this policy must follow the procedures for planning and justifying such projects specified in SAM Sections 4819.34 through 4819.42. <http://sam.dgs.ca.gov/TOC/4800/4819.34.htm>

Computing assets acquired as part of a previously approved IT project are incorporated into the Department's infrastructure and may be included in the desktop and mobile computing policy. All units and programs within CAL FIRE are subject to this policy.

DESKTOP AND MOBILE COMPUTING ORGANIZATIONAL RESPONSIBILITIES

960.1.4

(No.24 December 2009)

CAL FIRE Information Security Office (ISO)

The CAL FIRE ISO has responsibility for the development and maintenance of the software and hardware security policy.

The CAL FIRE ISO is responsible for reviewing Desktop and Mobile Computing acquisition requests involving the storage and maintenance of personal or confidential data to determine compliance with the California Records Act (Government Code 6250-6270), state regulations (SAM section 5315-5350.4), and federal laws. The ISO will ensure that appropriate controls are included to protect personal and confidential data.

The CAL FIRE ISO will audit the adequacy of safeguards and controls, and the achievement of system objectives in department personal computing systems. The Office of Program Accountability will also determine the extent of automated system compliance with recognized standards, policies, procedures, state regulations (SAM 5300), and federal laws and regulations.

CAL FIRE Management Responsibility

- The department has a current information management strategy and a current or planned information technology infrastructure description on file.
- The department has a standards policy, which controls the applications to be placed on desktop and mobile computing configurations.
- The department has a maintenance policy for computer assets used in desktop and mobile computing configurations.
- The department has the necessary standards and policies in place for the technical support of LAN activities, including installation, configuration, problem-determination, maintenance, backup, recovery and all other activities which would be in addition to those normally associated with stand-alone personal computers.

CAL FIRE Manager and Supervisor Responsibility

Managers and Supervisors are responsible for personnel within their units and their use of desktop and mobile computing assets, as well as for the security of associated data, equipment, and software whether in transit or storage. Desktop and mobile computing assets are considered a Departmental resource; as such they may be assigned for the exclusive use of an individual or unit within the Department; though such assignments may be changed at any time. Additionally, managers and supervisors are responsible to ensure that inventories are maintained in a manner consistent with SAM 8652 requirements.

Managers and Supervisors requesting to acquire desktop and mobile computing assets are responsible to ensure ongoing support funding is available and that equipment lifecycle issues are addressed prior to the acquisition.

CAL FIRE Desktop and Mobile Computing Coordinator

Responsibility for desktop and mobile computing coordination and technical assistance has been assigned to Information Technology Services (ITS) Customer Services Manager. Included in the responsibilities of the CAL FIRE Desktop and Mobile Computing Coordinator (DMCC) are the following functions:

- Assist with specifications for the Department's desktop and mobile computing Standard Procurement List.
- Assist in the completion and review of any DMCP documents if required by the Department's policies and procedures.
- Approve, sign and maintain a copy of desktop and mobile computing justification documentation for all items on the Department approved standard procurement list.
- Provide information to desktop and mobile computing users of available training and technical support capabilities.
- Ensure that proposed desktop and mobile computing applications are consistent with the Department's established information management strategy and information technology infrastructure and desktop and mobile computing configurations can support the implementation of other department applications.
- Oversee and manage the inventory of desktop and mobile computing assets.
- In conjunction with asset management, the desktop and mobile computing coordinator, Information Technology Services, will track workstation software licensing to ensure that all software in use by the Department is legal and appropriate.

CAL FIRE IT Coordinator/Customer Service Staff Responsibility

CAL FIRE utilizes IT Customer Service staff and IT Field Coordinators as the primary contact for users on all matters concerning the acquisition and use of desktop and mobile computing and network coordination within ITS.

CAL FIRE User Responsibility

Users must comply with State and Department policies governing the use of desktop and mobile computing assets within CAL FIRE.

CAL FIRE DESKTOP AND MOBILE COMPUTING POLICIES

960.1.5

(No.24 December 2009)

Procurement and Asset Management

All IT and Telecom procurement for CAL FIRE shall be governed by the Chief Information Officer. All IT and Telecom procurements shall conform to IT standards, procurement practices, and asset management policy and procedures.

All IT and Telecom products that are purchased, regardless of funding source (CAL FIRE, Cooperator, or grant) shall adhere to CAL FIRE policies and procedures for IT and Telecom acquisition.

All IT and Telecom assets procured shall be consistent with Technology Architecture principles defined by CAL FIRE Information Technology and the Telecom unit.

All IT assets used within the CAL FIRE computing environment shall conform to a set of standard operating environments prepared by Information Technology. Exemptions from the standard operating environments may be granted by the CIO, but only after the request for the exemption has been endorsed by the responsible manager.

Proposed systems, whether purchased, developed by an outside contractor, or developed by a CAL FIRE cooperator must be approved in advance by the Chief Information Officer.

Standards and Conventions

All IT products used within the CAL FIRE computing environment will adhere to standards and conventions as published by the CAL FIRE CIO.

Standard Procurement List of Approved Desktop and Mobile Computing Assets

The Desktop and Mobile Computing Coordinator in conjunction with ITS Procurement and Enterprise Architecture, develops the department approved, Standard Procurement List for desktop and mobile computing. Units proposing to acquire assets for desktop and mobile computing are expected to select from the standard procurement list. Requests to acquire items not included on the list require submittal of a special justification and approval by Information Technology Services.

Items on the Standard Procurement List have been selected from the Strategic Source Contracts provided by Department of General Services because they are of proven capability and reliability, are appropriately priced, and are compatible with configurations already in use in CAL FIRE. Minimum standards will be added to the Standard Procurement List in response to changing technology and State experience. It is CAL FIRE's policy to support a sufficiently wide range of hardware and software to accommodate a wide range of user needs.

The Standard Procurement List is available on the CAL FIRE Intranet.

<http://cdfweb/Its/ITSProcurementDocs/Standards.xls>

CAL FIRE Development of Software for Desktop and Mobile Computing

It is CAL FIRE policy to use commercial off-the-shelf (COTS) software rather than undertake independent software development. Fully tested and documented COTS software is readily available for most applications and usually more cost effective than custom-developed programs. Computer programming does not fall within this policy and must be justified in accordance with the requirements of SAM Sections 4819.3 through 4819.42.

Requests for custom software development require a Feasibility Study Report, project vision/scope document, and prior approval by the CIO. All custom developed software must follow ITS guidelines for structured development and documentation. Software developed for CAL FIRE becomes the property of CAL FIRE.

CAL FIRE Approval of Acquisition

Each request for acquisition of computer assets for a desktop and mobile computing configuration is subject to management review and approval before the order can be placed. The desktop and mobile computing request form, available on the CAL FIRE intranet <http://cdfweb/Its/ITSProcurementDocs/ITS-004%20PCRJ%20form.xls> provides for necessary approval signatures and certifications.

The review and approval procedure ensures that the proposed configuration conforms to established standards and satisfies the needs for which it is being acquired.

Acquisition of additional computer assets for previously acquired desktop and mobile computing configurations is also subject to similar review and approval.

Unit management is responsible for approval of the proposed acquisition of computer assets for desktop and mobile computing from the Standard Procurement List. The acquisition of IT assets for desktop and mobile computing must be in conformance with the applicable sections of the Public Contract Code, the State Administrative Manual and the Purchasing Authority Manual.

The amount of information and degree of detail provided must be commensurate with the nature, complexity, risk and expected cost of the proposed desktop and mobile computing effort. When such applications include the use of LAN components, such as servers or other shared devices, consideration and justification must be included for the necessary technical support for such activities as installation, configuration, problem-determination, maintenance, backup, recovery and all other activities which are in addition to those normally associated with stand-alone personal computers.

Post-Implementation Evaluation (PIER)

A post-implementation evaluation is not required for acquisitions under the desktop and mobile computing policy. A PIER is required for information technology projects and must be commensurate with the scope and complexity of the project and its anticipated benefits. SAM section 4947 through 4947.2 details the procedure for requirements of the PIER. <http://sam.dgs.ca.gov/TOC/4800/4947.htm>

Security, Confidential and Sensitive Information

Proposals to use desktop and mobile computing to maintain or access files containing confidential or sensitive data, as defined in SAM Section 5320.5 must be approved by the Department's Information Security Officer (SAM Section 5315.1). The Information Security Officer will determine if the proposal complies with all applicable provisions of the State Administrative Manual related to information security and risk management (Sections 5300 through 5305).

When information from desktop and mobile computing or network files are used to develop reports for distribution outside CAL FIRE or in the official recording of fiscal or personnel transactions, particular care must be taken to ensure the data is complete and accurate.

Questions regarding Information Security should be directed to the Information Security Officer in the Office of Program Accountability.

Integrity of Information

Information maintained by desktop and mobile computing configurations is subject to the same degree of management control and verification of accuracy that is provided for information maintained in other automated and manual files.

System Backup – Operational Recovery Plan

Provisions shall be made to ensure against the loss of data and programs stored in desktop and mobile computing configurations as a result of product failures or power failures. Copies of all data files and software shall be stored in a safe location. A regular schedule for making backup copies of all data files shall be established. Unit management shall ensure that backup procedures are carried out. Training in backup operations and procedures will be provided to unit management upon request.

Proprietary Software

In compliance with Governor's Executive Order D-10-99 and the SAM, CAL FIRE Information Technology Services' software license agreements shall be strictly adhered to. Proprietary software cannot be duplicated, modified, or used on more than one machine, except as expressly provided for in the manufacturer's license agreement.

Equipment and Software Documentation

Complete documentation shall be maintained for all the computer assets used for desktop and mobile computing. Documentation must include:

- Equipment and software manuals related to the installation, maintenance, care and use of equipment.
- Proprietary software shall be maintained with the equipment or in a central location, as appropriate.
- Each application (including database systems, spreadsheet software, or any software that maintains data files) shall have procedural documentation sufficient to allow productive use of the application in the absence of its primary user. This documentation will normally consist of the following:
 - User instructions documenting the scope and purpose of the application;
 - Specific data entry and processing instructions for the application;
 - System configuration information
 - Location software is installed (local machine, network, etc.)
 - Retention of data including back up and recovery
 - Passwords

Note: Network documentation is the responsibility of the Network Supervisor.

Training

User management is responsible to ensure that staff members possess the knowledge and skills necessary for effective use of desktop and mobile computing facilities and that there is sufficient depth of staff training to prevent disruption of key activities in the event of unexpected staff changes.

Staff members should be trained in each desktop and mobile computing application and the equipment they use.

The Desktop and Mobile Computing Coordinator (DMCC) is charged with providing lists of appropriate training materials or providers for all COTS software supported by CAL FIRE.

Maintenance and Repair

Each Unit within CAL FIRE will make provisions for necessary routine preventive maintenance, as well as for the repair of malfunctioning equipment. Problems with the operation of desktop and mobile computing equipment or a network should be reported first to the CAL FIRE Help Desk, who will arrange for appropriate repairs according to established procedures. If the Help Desk cannot resolve the problem, the Help Desk will notify the appropriate Field IT Coordinator.

Inventory of Computer Assets and Applications

CAL FIRE Information Technology Services will maintain an inventory of CAL FIRE's significant computer assets used for desktop and mobile computing configurations using an asset management system as required by SAM Section 8652. The inventory will provide a description of each item (including serial, model, and State property sticker numbers of equipment and version numbers of software), its date of acquisition, and the unit to which it is currently assigned. CAL FIRE ITS will maintain inventories of licensed software and significant applications installed on desktop and mobile computing configurations. These inventories are available for audit purposes.

LEGAL OBLIGATIONS

960.1.6

(No.24 December 2009)

In our role as employees of CAL FIRE and as individuals responsible for data processing on mainframe or desktop and mobile computing, we have legal and professional obligations to protect the data, which has been entrusted to us for processing. It is the responsibility of every employee who works with computers to understand these obligations and to ensure that they are followed. Data residing on desktop and mobile computing equipment is subject to the same restrictions and guidelines regarding security and accuracy as data residing on a mainframe. Refer to the 0900 Acceptable Use Policy section of the ITS Handbook.

<http://calfireweb/library/handbooks/0900/0911.pdf> .

[\(see HB Table of Contents\)](#)

[\(see Forms and Form Samples\)](#)